IN THE CLAIMS

Please cancel claims 1-5 and substitute the following new claims 6-10.

What is claimed is:

1. (cancelled) A wide area network using the internet as a backbone, comprising:

a first dedicated line coupled to a first participating ISX/ISP provider of internet access;

a source router having a channel service unit having an output coupled to said first dedicated line;

a source firewall circuit having a first port for coupling directly or through a local area network to a first device for which communication over said wide area network (hereafter WAN) is desired, and having a WAN interface coupled to said source router directly or through a local area network, said source firewall functioning to encrypt the payloads of downstream WAN packets being transmitted via the WAN interface to said source router using any encryption method having a user definable key or keys, and for decrypting the payloads of any incoming upstream WAN packets arriving from said source router via said WAN interface using the same encryption method and user definable key or keys that were used to encrypt the outgoing WAN packets;

one or more routers of other participating ISX/ISP providers of internet services including a router at an endpoint participating ISX/ISP provider, said routers functioning to implement a predetermined private tunnel data path coupling a router of said first ISX/ISP to a router of said endpoint participating ISX/ISP provider through said routers of said participating ISX/ISP providers;

a destination router including a channel service unit coupled to or part of said destination router, said destination router coupled through said channel service unit and a second dedicated line to said router of said endpoint ISX/ISP provider;

a destination firewall circuit having a WAN interface coupled to said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to a device for which communication across said wide area network is desired, said firewall

functioning to encrypt the payloads of upstream WAN packets being transmitted through said WAN interface to said destination router for transmission to said source router via said private tunnel using the same encryption method used by said source firewall and the same user definable key or keys used by said source firewall circuit, and for decrypting any incoming packets from said source router arriving from said endpoint participating ISX/ISP provider using the same encryption protocol used by said source firewall and the same user definable key or keys used by said source firewall circuit and transmitting the decrypted packets to said second device.

2. (cancelled) A process for launching downstream AlterWAN packets addressed to an AlterWAN destination into a private tunnel coupling two AlterWAN destinations using the internet as a backbone and for launching non-AlterWAN packets into a normal internet traffic routing data path, comprising the steps:

receiving at a source firewall an incoming downstream wide area network packet from a workstation or other device at a first customer location said incoming downstream wide area network packet being either addressed to an AlterWAN destination or not an AlterWAN packet;

at said source firewall, using the destination address in said incoming downstream wide area network packet to determine if said packet is addressed to an AlterWAN destination coupled to said source firewall by a private tunnel using the internet as a backbone (hereafter referred to as an AlterWAN packet) or is addressed to some non-AlterWAN website or location on the internet (hereafter referred to as a non-AlterWAN packet);

if said packet is an AlterWAN packet, encrypting at said source firewall the payload portion thereof and forwarding the encrypted AlterWAN packet to a source router;

if said packet is a non-AlterWAN packet, at said source firewall, forwarding said non-AlterWAN packet to said source router without encrypting the payload portion thereof;

at said source router, converting both said AlterWAN packets and said non-AlterWAN packets into signals suitable for transmission on a dedicated telephone line or other transmission medium coupling said source router to a

specially selected first ISX/ISP provider and transmitting said signals to said specially selected ISX/ISP provider, said specially selected ISX/ISP provider being selected either because their routing tables are such that AlterWAN packets will naturally be routed along high bandwidth, low hop-count data paths to the next ISX/ISP provider in said virtual private network or because the routing tables of the router of said first ISX/ISP provider have been altered to insure that AlterWAN packets get routed along high bandwidth, low hop-count data paths to the next ISX/ISP provider along said private tunnel.

3. (Cancelled) An apparatus comprising:

a dedicated data path for coupling to a specially selected first participating ISX/ISP provider of internet access;

a firewall circuit having a first port for coupling directly or through a local area network to one or more devices for which communication over a wide area network using the internet as a backbone is desired, and having a second port, said firewall functioning to to use the destination addresses in the headers of each packet received from said one or more devices to distinguish between AlterWAN packets which are packets addressed to destination devices coupled to said firewall circuit via a private tunnel through the internet, and conventional packets which are packets not addressed to destination devices coupled to said firewall circuit via a private tunnel through the internet, said firewall circuit functioning to encrypt the payloads of outgoing AlterWAN packets using one or more predetermined keys and an encryption algorithem, and sending said encrypted AlterWAN packets to said source router via said second port, and functioning to forward any conventional packets to said source router, and functioning to decrypt any incoming AlterWAN packets arriving from said source router using the the same encryption algorithms and one or more predetermined keys which were used to encrypt the packets at the location from which they were sent;

a source router having an input coupled to said second port of said firewall circuit either directly or by a local area network connection, and having a channel service unit having an output coupled to said dedicated data path, said channel service unit functioning to convert digital data packets received from said

firewall circuit into signals suitable for transmission over whatever type of transmission medium is selected for said dedicated data path, and for converting signals received from said dedicated data path into data packets, said source router for transmitting both AlterWAN and non-AlterWAN packets over said dedicated data path to said specially selected first participating ISX/ISP provider where AlterWAN packets will be routed via said private tunnel and specially seleted ISX/ISP providers to their destination and non-AlterWAN packets will be routed along paths on the internet other than said private tunnel.

4. (Cancelled) A method of designing and implementing a wide area network using the internet as a backbone, comprising the steps:

1) selecting source and destination sites that have devices that need to be connected by a wide area network;

2) examining the ISX/ISP internet service providers that exist between said source and destination sites and selecting two or more of such ISX/ISP providers through which data passing between said source and destination sites will be routed, said selection being based upon how many hops the routers at those sites will cause packets travelling between said source and destination sites to take and whether the average available bandwidth of the data paths along which the packets travelling between said source and destination sites will travel is substantially greater than the worst case bandwidth consumption of traffic between said source and destination sites;

3) coupling a source firewall to the devices at said source site and configuring said firewall to examine the destination addresses of packets received from said devices at said source site and encapsulate each packet addressed to any device at said destination site in an internet protocol packet, hereafter referred to as an AlterWAN packet, said AlterWAN packet having as its destination address the address of an untrusted port of a destination firewall at said destination site and having the original IP packet as its payload, said source firewall being configured to encrypt the payload portions of all said AlterWAN packets using a predetermined encryption algorithm and one or more encryption keys but not to encapsulate or encrypt the payload portions of any packets received from said devices at said source site which are not addressed to any

device at said destination site, and configuring said source firewall to recognize any incoming AlterWAN packets which have as their destination addresses the IP address of the untrusted side of said source firewall and to strip off the AlterWAN packet headers and decrypt the payload portion of each said AlterWAN packet to recover the original IP packet transmitted from said destination site using the same encryption algorithm and the same encryption key or keys used to encrypt the payload portions of said AlterWAN packets at said destination site and for outputting said recovered the original IP packet to said devices at said source site, said source firewall having an untrusted port;

4) coupling a source router to receive said encrypted and non-encrypted packets from said untrusted port of said source firewall and to convert them in a channel service unit to signals suitable for transmission over a first dedicated local loop connection;

5) contracting to establish said first dedicated local loop connection between the output of said source router at which said signals appear and a first participating ISX/ISP provider in the group of ISX/ISP providers selected in step 2;

6) providing a destination router at said destination site having a channel service unit which functions to receive from a second dedicated local loop connection downstream signals encoding both encrypted AlterWAN packet and conventional IP packets and converting said signals back into the original digital packet form and outputting the recovered downstream packets at a firewall port, and said destination router configured to receive upstream AlterWAN and conventional packets and convert them into signals suitable for transmission on said second dedicated data path coupling said destination router to an endpoint participating ISX/ISP provider in the group of ISX/ISP providers selected in step 2 and transmitting said signals on said second dedicated local loop connection;

7) contracting to provide a second dedicated local loop connection connecting the input of said destination router to said endpoint participating ISX/ISP provider, said second dedicated local loop connection having sufficiently high bandwidth to handle the worst case traffic volume;

8) providing a destination firewall having an untrusted port having an IP address coupled to said firewall port of said destination router to receive said recovered digital packets, and configuring said destination firewall to recognize

as AlterWAN packets incoming recovered packets having as their destination address the IP address of said destination firewall untrusted input port and to strip off the AlterWAN packet header and decrypt the payload portion of said AlterWAN packet using the same encryption algorithm and encryption key or keys that were used to encrypt the packet at said source firewall, and configuring said destination firewall to output the decrypted packets at an output coupled to devices at said destination site, and configuring said destination firewall to examine the destination addresses of upstream IP packets received from said devices at said destination site and encapsulate each upstream IP packet addressed to any device at said source site in another IP packet, hereafter referred to as an AlterWAN packet, said AlterWAN packet having as its destination address the IP address of an untrusted port of said source firewall at said source site and having the original IP packet as its payload, said destination firewall being configured to encrypt the payload portions of all said AlterWAN packets using a predetermined encryption algorithm and one or more encryption keys but not to encapsulate or encrypt the payload portions of any IP packets received from said devices at said destination site which are not addressed to any device at said source site (hereafter referred to as conventional packets), and said destination firewall configured to transmit said encrypted AlterWAN packets and said conventional packets to said destination router via said untrusted port.

5. (Cancelled) A wide area network using the internet as a backbone, comprising:

a first dedicated line coupled to a first participating ISX/ISP provider of internet access;

a source router having a channel service unit having an output coupled to said first dedicated line;

a source firewall circuit having a first port for coupling directly or through a local area network to a first device for which communication over said wide area network (hereafter WAN) is desired, and having a WAN interface coupled to said source router directly or through a local area network, said source firewall functioning to encrypt the payloads of downstream WAN packets being

transmitted via the WAN interface to said source router using a first encryption method having a first set of user definable keys which may be only one key, and for decrypting the payloads of any incoming upstream WAN packets arriving from said first participating ISX/ISP using a second encryption method which is different than said first encryption method and a second set of user definable keys which are different than the first set of user definable keys were used to encrypt the downstream WAN packets;

one or more routers of other participating ISX/ISP providers of internet services including a router at an endpoint participating ISX/ISP provider, said routers functioning to implement a predetermined private tunnel data path coupling a router of said first ISX/ISP to a router of said endpoint participating ISX/ISP provider through said routers of said participating ISX/ISP providers;

a destination router including a channel service unit coupled to or part of said destination router, said destination router coupled through said channel service unit and a second dedicated line to said router of said endpoint ISX/ISP provider;

a destination firewall circuit having a WAN interface coupled to said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to a device for which communication across said wide area network is desired, said destination firewall functioning to encrypt the payloads of upstream WAN packets being transmitted through said WAN interface to said destination router for transmission to said source router via said private tunnel using the same encryption method and user definable key or keys used by said source firewall to decrypt upstream WAN packets, and for decrypting any incoming downstream WAN packets from said source router arriving from said destination router via the router of said endpoint participating ISX/ISP provider using the same encryption method and encryption key or keys used by said source firewall to encrypt downstream WAN packets and transmitting the decrypted packets to said second device.

6. (New) A private, secure wide area network between a source site and a destination site using the internet as a backbone, comprising:

a first dedicated local loop connection providing a signal path to a router of a

source ISX/ISP provider of internet access;

a source router located at a source site and having a channel service unit having an output coupled to said first dedicated local loop connection;

a source firewall circuit located at a source site and having a first port for coupling directly or through a local area network to one or more computers or other devices at said source site for which communication over said private, secure wide area network (hereafter WAN) is desired, and having a WAN interface coupled to said source router directly or through a local area network, said source firewall functioning to encapsulate any Internet Protocol packets hereafter IP packets transmitted from said first computer or other device which have a destination Internet Protocol address (hereafter IP address) which is one of a set of IP addresses of computers or other devices at a destination site, said encapsulation being into the payload sections of IP packets having as their destination address the IP address of a firewall at said destination site and for encrypting said payload sections of said AlterWAN packets using any encryption method having a key, and transmitting said AlterWAN packets to said source router, where IP packets having as their destination address the IP address of a computer or other device at either said source site or said destination site and having an encrypted IP packet transmitted from a computer or other device at said source site or said destination site as a payload being defined and hereafter referred to as AlterWAN packets, but for not encapsulating into AlterWAN packets any IP packets transmitted by said first computer or other device which do not have as their destination address an IP address which is one of said IP addresses of computers or other devices at said destination site, and for receiving incoming IP packets from various sources including computers and devices at said destination site via said source router and for recognizing AlterWAN packets among these IP packets and decrypting the payloads of said AlterWAN packets using the same encryption method and key or keys that were used to encrypt the AlterWAN packets to recover said IP packets that were encapsulated in said AlterWAN packets and transmitting at least said recovered IP packets to said one or more computers or devices at said source site;

one or more routers of other participating ISX/ISP providers of internet services besides said source ISX/ISP provider including a router at an endpoint participating ISX/ISP provider, said routers of said source and endpoint ISX/ISP

providers and said other participating ISX/ISP providers functioning to implement a predetermined private tunnel data path for said AlterWAN packets coupling a router of said source ISX/ISP provider to a router of said endpoint participating ISX/ISP provider through said routers of said other participating ISX/ISP providers, said source and endpoint ISX/ISP providers and said other ISX/ISP providers being providers of internet services who have contracted to provide and who have been pretested to verify that they do in fact provide a low hop count portion of a data path between said source site and said destination site for said AlterWAN packets with an average available bandwidth along said portion of said data path travelled by said AlterWAN packet which each ISX/ISP provider provides which substantially exceeds the worst case bandwidth consumption of AlterWAN packet traffic between said source site and said destination site;

a destination router including a channel service unit coupled to or part of said destination router, said destination router coupled through said channel service unit and a second dedicated local loop connection to said router of said endpoint ISX/ISP provider;

a destination firewall circuit having a WAN interface coupled to said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to a one or more computers or devices for which communication across said private, secure wide area network is desired, said destination firewall functioning to encapsulate into the payload sections of AlterWAN packets IP packets transmitted from said one or more computers or devices at said destination site and having as their destination addresses an IP address of said one or more computers or devices at said source site, and functioning to encrypt the payloads of said AlterWAN packets and transmit said AlterWAN packets to said destination router, but for not encapsulating into AlterWAN packets any IP packets transmitted from said one or more computers or devices at said destination site which do not have as their destination address an IP address of said one or more computers or devices at said source site, and for receiving IP packets from various sources including said one or more computers or devices at said source site via said destination router, and functioning to recognize AlterWAN packets among said received IP packets and decrypt the payload sections of said AlterWAN packets to recover the original IP packets using the same encryption

protocol used by said source firewall to encrypt said payload sections of said AlterWAN packets and the same key or keys used by said source firewall and transmitting at least the decrypted IP packets recovered from AlterWAN packet to said one or more computers or devices at said destination site.

7. (New) A process for sending AlterWAN data packets securely between a computer at a source site and a computer at a destination site so as to implement a Wide Area Network between said source and destination sites of a customer using the internet as a backbone but which is private and which only said customer can use while simultaneously launching non-AlterWAN packets into a normal internet traffic routing data path, comprising the steps:

receiving at a source firewall incoming Internet Protocol packets (hereafter IP packets) from a computers at a source site of a customer, some of said IP packets having as their destination addresses an Internet Protocol address (hereafter IP address) of a computer at a destination site of said customer;

at said source firewall, comparing the destination address in each said received IP packet to an IP address of a computer at said destination site of said customer, and if an IP packet has as its destination address the IP address of a computer at said destination site, concluding said IP packet is an AlterWAN packet payload which needs to be transmitted via a virtual private network over the internet to said computer at said destination site, but if said destination address of said received IP packet is not an IP address of a computer at said destination site, concluding said IP packet is nont an AlterWAN payload packet and needs to be routed as any other IP packet would be routed;

if a received IP packet is an AlterWAN payload packet, encapsulating said AlterWAN payload packet into the payload section of an IP packet having as its destination address the IP address of a firewall at the destination end of said virtual private network (hereafter referred to as AlterWAN packet) and encrypting at said source firewall the payload portion of said AlterWAN packet using any encryption algorithm having a key which same encryption algorithm and key can be used by a firewall at said destination site to recover said AlterWAN payload packet, and forwarding said AlterWAN packet to a source router;

if a received IP packet is not an AlterWAN payload packet,forwarding said

received IP packet which is not an AlterWAN payload packet (hereafter referred to as a non-AlterWAN packet) to said source router without encapsulating said non-AlterWAN packet into an AlterWAN packet;

at said source router, converting both said AlterWAN packets and said non-AlterWAN packets into signals suitable for transmission on a dedicated local loop connection coupling said source router to a specially selected source participating ISX/ISP provider and transmitting said signals to said specially selected source participating ISX/ISP provider, said specially selected source participating ISX/ISP provider being selected either because their routing tables are such that AlterWAN packets will naturally be routed along high bandwidth, low hop-count data paths to next participating ISX/ISP provider in said virtual private network or because the routing tables of the router of said specially selected source participating ISX/ISP provider have been altered to insure that AlterWAN packets get routed along high bandwidth, low hop-count data paths to the next ISX/ISP provider along said virtual private network and wherein said source participating ISX/ISP provider and all other participating ISX/ISP providers whose routers route AlterWAN packets have contracted to provide a data path for said AlterWAN packets with an average available bandwidth which exceeds the worst case bandwidth consumption of AlterWAN packets traveling between said source site and said destination site of said customer.

8. (New) An apparatus comprising:

a dedicated data path for coupling signals to a specially selected first participating ISX/ISP provider of internet access;

a first firewall circuit having a first port for coupling directly or through a local area network to one or more devices for which communication over a private wide area network between a customer's source site and destination site using the internet as a backbone is desired, and having a second port, said firewall functioning to use the destination addresses in the headers of each packet received from one or more devices at said source site to distinguish between conventional packets and AlterWAN payload packets, where AlterWAN payload packets are packets addressed to devices at said destination site or said source site, and wherein a computer at said destination site is coupled to a computer at said source site via a

second firewall circuit and a virtual private network tunnel through a public wide area network such as the internet terminating at said source site at said first firewall circuit and terminating at said destination site at said second firewall circuit, and wherein conventional packets are packets which are not addressed to devices at said destination site said first firewall circuit functioning to encapsulate said AlterWAN payload packets in the payload section of AlterWAN packets which are addressed to said second firewall circuit at said destination end of said virtual private network tunnel, and further functioning to encrypt the payloads of AlterWAN packets using one or more predetermined keys and an encryption algorithm, and said first firewall circuit further functioning to distinguish between incoming AlterWAN packets and conventional packets by comparing the destination addresses thereof to the address of said first firewall circuit and concluding that any incoming packets addressed to said first firewall circuit are AlterWAN packet and all packets addressed to one or more computers at said source site coupled to said first firewall circuit are conventional packets, and to decrypt the payload sections of any incoming AlterWAN packets using the same encryption algorithm and one or more predetermined keys which were used to encrypt the AlterWAN packets so as to recover the encapsulated AlterWAN payload packet;

a source router having an input coupled to said second port of said firewall circuit either directly or by a local area network connection, and having a channel service unit having an output coupled to said dedicated data path, said router and channel service unit functioning to receive said AlterWAN packets and said conventional packets from said first firewall circuit and convert said packets into signals suitable for transmission over whatever type of transmission medium is selected for said dedicated data path, and for converting signals received from said dedicated data path into data packets, said source router for transmitting both AlterWAN packets and conventional packets over said dedicated data path to said specially selected first participating ISX/ISP provider where said AlterWAN packets will be routed via said virtual private network tunnel and specially selected participating ISX/ISP providers to said second firewall and non-AlterWAN packets will be routed along paths on the internet other than said virtual private network tunnel and wherein said first participating ISX/ISP provider and all said other ISX/ISP providers are providers who have contracted to and do in fact provide data paths for

AlterWAN packets which combine to form a low hop count data path with an average available bandwidth which substantially exceeds the worst case bandwidth consumption of AlterWAN packets traveling between said source site and said destination site.

9. (New) A method of designing and implementing a wide area network using the internet as a backbone, comprising the steps:

1) selecting source and destination sites that have computers or other devices (hereafter referred to simply as computers) that need to be connected by a wide area network;

2) examining available ISX/ISP internet service providers that can route AlterWAN packets between said source and destination sites and selecting two or more of such ISX/ISP providers as participating ISX/ISP providers including at least a source ISX/ISP provider and a destination ISX/ISP provider through which AlterWAN packet data passing between said source and destination sites will be routed, said selection of said participating ISX/ISP providers being made so as to minimize the number of hops on the internet the routers at participating ISX/ISP providers will cause AlterWAN packets to take while traveling between said source and destination sites and so as to guarantee that the average available bandwidth of the data paths along which said AlterWAN packets traveling between computers at said source and destination sites will travel is substantially greater than the worst case bandwidth consumption of traffic between said source and destination sites;

3) pretesting the ISX/ISP providers selected in step 2 by testing to verify the data path that an AlterWAN packets will take through the internet to verify that what the participating ISX/ISP providers promised to deliver will actually be delivered;

4) contracting with said participating ISX/ISP providers to provide routing of AlterWAN packets so as to minimize the number of hops on the internet said AlterWAN packets need to take in traveling between said source and destination sites and so as to guarantee that the average available bandwidth along data paths AlterWAN packets must traverse to travel between said source and destination sites is substantially greater than the worst case bandwidth consumption of traffic between source and destination sites, and, if necessary, configuring data in routing tables of said participating ISX/ISP providers so as to minimize said number of hops

and guarantee said bandwidth contracted for when routing AlterWAN packets;

5) contracting to establish a first dedicated local loop connection between the output of a source router at which said signals appear and said source ISX/ISP provider in the group of ISX/ISP providers selected in step 2, said first dedicated local loop connection having sufficiently high bandwidth to handle the worst case traffic volume in AlterWAN packets traveling between said source and destination sites;

6) contracting to provide a second dedicated local loop connection connecting the input of a destination router to said destination ISX/ISP provider, said second dedicated local loop connection having sufficiently high bandwidth to handle the worst case traffic volume in AlterWAN packets traveling between said source and destination sites;

7) coupling an untrusted port of a source firewall/virtual private network circuit (hereafter referred to as the source firewall) to a source router and coupling a trusted port of said source firewall to said device or devices at said source site and configuring said source firewall to examine the destination addresses of internet Protocol packets (hereafter IP packets) received from said devices at said source site and encapsulate each IP packet having a destination address which is the Internet Protocol address (hereafter IP address) of any device at said destination site as a payload portion in a second IP packet, hereafter referred to as an AlterWAN packet, said AlterWAN packet having as its destination address the IP address of an untrusted port of a destination firewall/virtual private network circuit (hereafter referred to as the destination firewall) at said destination site and having the original IP packet as its payload with portions of said AlterWAN packet other than said payload section being referred to herein as an AlterWAN packet header, said source firewall also being configured to encrypt the payload portions of all said AlterWAN packets using a predetermined encryption algorithm and one or more encryption keys but not to encapsulate or encrypt the payload portions of any packets received from said devices at said source site which do not have as their destination address the IP address of any device at said destination site (hereafter referred to as non AlterWAN packets), and configuring said source firewall to screen incoming IP packets so as to recognize any incoming AlterWAN packets which have as their destination addresses the IP address of the untrusted port of said source firewall and to strip off the AlterWAN packet headers and decrypt the payload portion of each said incoming

AlterWAN packet to recover the original IP packet transmitted from said destination firewall using the same encryption algorithm and the same encryption key or keys used to encrypt the payload portions of said AlterWAN packets when they were transmitted from said destination firewall so as to recover the original IP packet transmitted to said destination firewall by a computer at said destination site; and for outputting said recovered original IP packet to said device or devices at said source site having the IP address which is the destination address of said original IP packet;

8) coupling a source router to receive said encrypted AlterWAN packets and non-encrypted non-AlterWAN packets from said untrusted port of said source firewall and to convert said AlterWAN and non-AlterWAN packets in a channel service unit to signals suitable for transmission over said first dedicated local loop connection to said source ISX/ISP provider;

9) providing a destination router at said destination site having a firewall port coupled to said untrusted port of said destination firewall and having a channel service unit coupled to said destination ISX/ISP provider via said second dedicated local loop connection and which is configured to receive from said second dedicated local loop connection downstream signals encoding both encrypted AlterWAN packets and conventional non AlterWAN IP packets and converting said signals back into the original digital IP packet form and configuring said destination router to output said recovered downstream IP packets at said firewall port coupled to said untrusted port of said destination firewall, and said destination router configured to receive upstream AlterWAN packets and conventional non AlterWAN packets and convert both types of said packets into signals suitable for transmission on said second dedicated local loop connection coupling said destination router to said participating destination ISX/ISP provider in the group of participating ISX/ISP providers selected in step 2 and transmitting said signals on said second dedicated local loop connection;

10) providing a destination firewall having an untrusted port coupled to said firewall port of said destination router so as to receive said recovered digital IP packets, and configuring said destination firewall to recognize as AlterWAN packets incoming recovered IP packets having as their destination address the IP address of said destination firewall untrusted port and further configured to strip off the AlterWAN packet header of each said AlterWAN packet and decrypt the payload portion of each said AlterWAN packet using the same encryption algorithm and

encryption key or keys that were used to encrypt the AlterWAN packet at said source firewall so as to recover the original IP packet encapsulated in each AlterWAN packet, and configuring said destination firewall to output the decrypted original IP packets at an output coupled to a device or devices at said destination site, and configuring said destination firewall to examine the destination addresses of upstream IP packets received from a device or devices at said destination site and encapsulate each upstream IP packet addressed to any computer or other device at said source site as the payload portion of in another IP packet, hereafter referred to as an upstream AlterWAN packet (an AlterWAN packet traveling from said destination site toward said source site), said AlterWAN packet having as its destination address the IP address of said untrusted port of said source firewall at said source site and having the original IP packet as its payload, said destination firewall being configured to encrypt the payload portions of all said upstream AlterWAN packets using a predetermined encryption algorithm and one or more encryption keys but not to encapsulate or encrypt the payload portions of any non AlterWAN IP packets received from said device or devices at said destination site which do not have as their destination addresses an IP address of any device at said source site (hereafter referred to as conventional non AlterWAN packets), and said destination firewall configured to transmit said encrypted upstream AlterWAN packets and said conventional non AlterWAN packets to said destination router via said untrusted port.

10. (New) A private wide area network connecting a customer source site to a customer destination site and using the internet as a backbone, comprising:

a first dedicated data path coupled to a first participating ISX/ISP provider of internet access;

a source router having a channel service unit having an output coupled to said first dedicated data path;

a source firewall circuit having a first port for coupling directly or through a local area network to one or more devices at a customer source site, and having an untrusted port coupled to said source router directly or through a local area network, said untrusted port of said source firewall having an Internet Protocol address (hereafter IP address), said source firewall functioning to receive Internet Protocol packets (hereafter IP packets) from said one or more devices at said customer

source site which are addressed to one or more devices at a customer destination site (hereafter AlterWAN payload packets) and other IP packets addressed to other locations on the internet (hereafter conventional IP packets), and for encapsulating said AlterWAN payload packets as the payload sections of IP packets addressed to an IP address of an untrusted port of a destination firewall at said customer destination site (hereafter outgoing AlterWAN packets) and functioning to encrypt the payloads of said outgoing AlterWAN packets using a first encryption method known to a destination firewall and using a key or key known to said destination firewall and which may be user definable, and for receiving incoming IP packets and comparing the destination addresses of said incoming IP packets to said IP address of said untrusted port of said source firewall circuit, and decrypting the payload sections of any incoming IP packets having as their destination address the IP address of said untrusted port of said source firewall circuit (hereafter incoming AlterWAN packets) using whatever encryption method and key or keys which were used to encrypt them so as to recover the encapsulated AlterWAN payload packet from each incoming AlterWAN packet, and transmitting each recovered AlterWAN payload packet to a device at said customer source site to which said AlterWAN payload packet is addressed;

one or more routers of other participating ISX/ISP providers of internet services including a router at an endpoint participating ISX/ISP provider, said routers of said ISX/ISP providers functioning to implement a low hop count data path in the form of a virtual private network tunnel through the internet coupling one or more devices at said customer source site to one or more computers at said customer destination site, said low hop count data path having an average available bandwidth which is substantially greater than the worst case bandwidth consumption of AlterWAN packets traveling between said customer source site and said customer destination site;

a destination router including a channel service unit coupled to or part of said destination router, said destination router coupled through said channel service unit and a second dedicated datapath to said router of said endpoint participating ISX/ISP provider;

a destination firewall circuit having an untrusted port having an IP address to which said outgoing AlterWAN packets are addressed, said untrusted port coupled to

said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to one or more devices at said customer destination site, said destination firewall circuit functioning to receive IP packets from said one or more devices at said customer destination site which are addressed to one or more devices at said customer source site (hereafter AlterWAN payload packets) and functioning to receive other conventional IP packets, and for encapsulating said AlterWAN payload packets as the payload sections of AlterWAN packets addressed to said IP address of an untrusted port of said source firewall circuit at said customer source site (hereafter outgoing AlterWAN packets) and functioning to encrypt the payloads of said outgoing AlterWAN packets using an encryption method known to said source firewall and a key or keys known to said source firewall and for receiving incoming IP packets and comparing the destination addresses of said incoming IP packets to said IP address of said untrusted port of said destination firewall circuit, and decrypting the payload sections of any incoming IP packets having as their destination address the IP address of said untrusted port of said destination firewall circuit (hereafter incoming AlterWAN packets) using whatever encryption method and key or keys which were used to encrypt said incoming AlterWAN packets so as to recover the encapsulated AlterWAN payload packet from each incoming AlterWAN packet, and transmitting each recovered AlterWAN payload packet to the device to which it is addressed at said customer destination site.